GROUPS OF SPECIAL GALOIS DOMAINS OF RATIONALITY

BY

HARRY ALBERT BENDER
A. B. Ohio University, 1918

THESIS

Submitted in Partial Fulfillment of the Requirements for the

Degree of

MASTER OF ARTS

IN MATHEMATICS

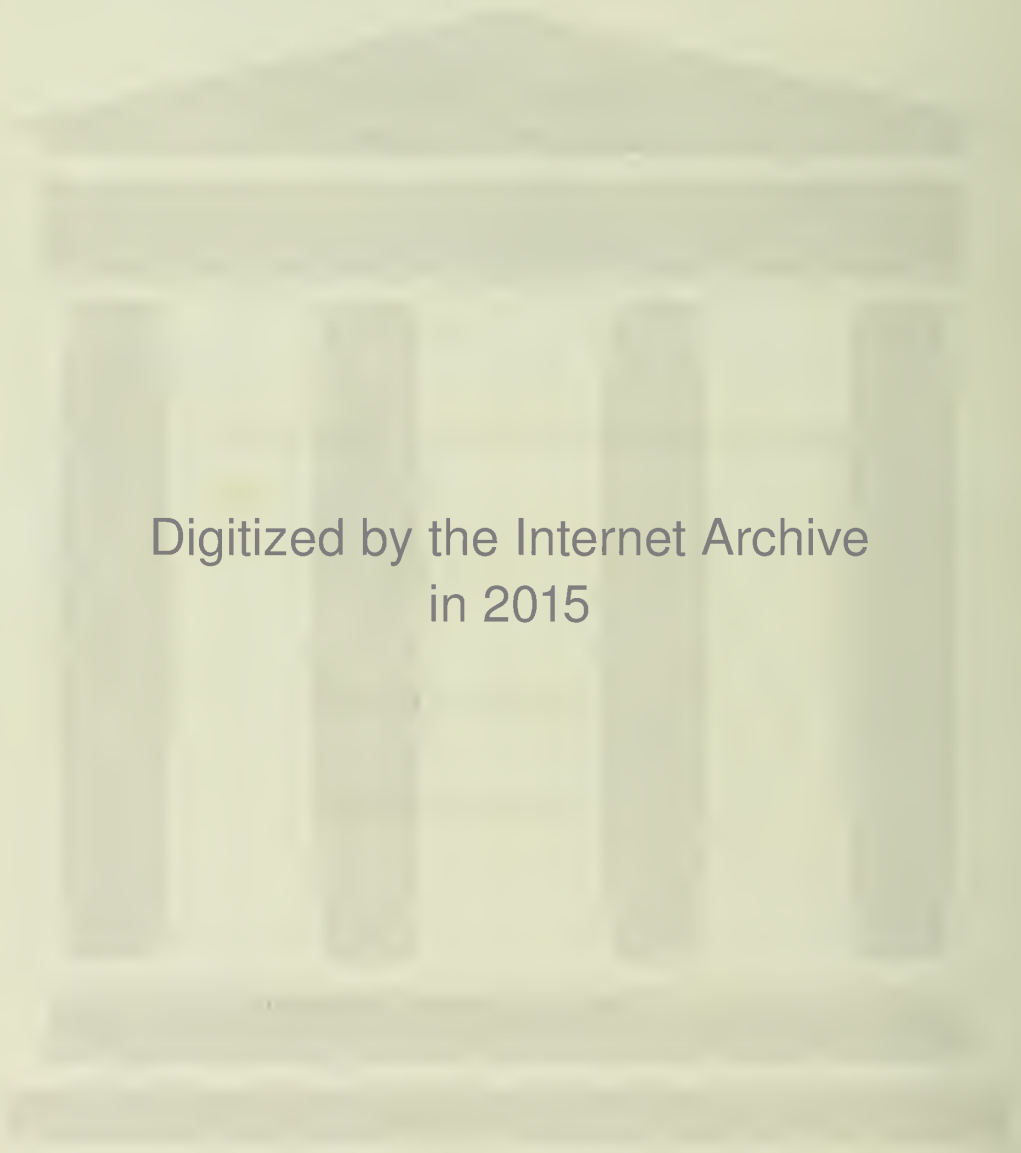
IN

THE GRADUATE SCHOOL

OF THE

UNIVERSITY OF ILLINOIS

1921



UNIVERSITY OF ILLINOIS

THE GRADUATE SCHOOL

July 28 1924

I HEREBY RECOMMEND THAT THE THESIS PREPARED UNDER MY SUPERVISION BY A. A. Bender

ENTITLED Groups of Special Galois-domains of Rationality

BE ACCEPTED AS FULFILLING THIS PART OF THE REQUIREMENTS FOR THE DEGREE OF Master of Arts.

G. E. Wahlin
In Charge of Thesis

A. B. Coble for E. J. Townsend.
Head of Department

Recommendation concurred in*

Committee on Final Examination*

*Required for doctor's degree but not for master's

Let $f(x)=0$ be an irreducible equation of degree n and let $x_1, x_2, x_3, \ldots\ldots, x_n$ be its roots. Let p* be an arbitrary rational prime and let us suppose that in k(p)

$$(1) \quad f(x)=f_1(x).f_2(x).f_3(x).\ldots\ldots.f_s(x) \quad (p)$$

where $f_i(x)$ is of degree n_i, and irreducible in k(p).

In k(p), the domain of the rational p-adic numbers, the number x_1 cannot satisfy an equation of degree less than n (x_1 is taken in this sense as any one of the roots of f(x)). For suppose that

$$\phi(x)=a_0 x^{n-1}+a_1 x^{n-2}+\ldots\ldots+a_{n-1}$$

is a polynomial of degree less than n, with p-adic coefficients, such that $\phi(x_1)=0$ (p), and let

$$x_1^{i-1}=a_{i1}w_1+a_{i2}w_2+\ldots\ldots+a_{in}w_n \quad (i=1,2,3,\ldots\ldots,n).$$

We then have

$$\phi(x_1)=A_1 w_1+A_2 w_2+\ldots\ldots+A_n w_n$$

$$A_i=a_0 a_{ni}+a_1 a_{n-i}+\ldots\ldots+a_{n-1}a_{1i} \quad (i=1,2,3,\ldots\ldots,n).$$

Since an integer of $k(x_1)$ is divisible by p when and only when each coefficient in its representation by a fundamental system is a multiple of p, we conclude that $\phi(x_1)=0$ (p) when and only when $A_i=0$ (p) $(i=1,2,3,\ldots\ldots,n)$, and from this system of equations it follows that $|a_{ij}|.a_\beta=0$ (p).

But the $a_{i\beta}$ are ordinary rational integers and hence $|a_{ij}|$ is a number of k(1) and since it is not zero there exists a

*By p without subscripts we shall mean an arbitrary rational prime, and p with subscripts we shall mean the prime divisors of p in the algebraic domain.

number $\left|\frac{1}{a_{ij}}\right| \neq 0$ and

$$\left|\frac{1}{a_{ij}}\right| \cdot |a_{ij}| \cdot a_k = a_k = 0 \ (p).$$

Hence $\phi(x)$ must vanish identically, and x_1 cannot in $k(p)$ satisfy an equation of degree less than n.

From (1) we have

$$f(x_1) = f_1(x_1) \cdot f_2(x_1) \cdot f_3(x_1) \cdot \text{--------} \cdot f_s(x_1) = 0 \ (p)$$

while no one of the factors is zero. We therefore conclude that in this case $R(p,x_1)$ is not a domain.

Since $f(x)$ is irreducible in the ordinary sense its discriminant cannot vanish and hence it must also be different from zero for the domain of p. Consequently no two of the s factors can be equal.

We shall now introduce, corresponding to each of the s factors of $f(x)$, s new systems of values for the numbers of $R(p,x_1)$ as follows. If $\beta = B(x_1)$ is any number of $R(p,x_1)$ and if

$$B(x) = Q_i(x) \cdot f_i(x) + R_i(x) \ (p),$$

we shall call $R_i(x_1)$ the value of β for the domain of p_i corresponding to the factor $f_i(x)$ and shall write $\beta = R_i(x_1) \ (p_i)$.

Two numbers $\beta_1 = B_1(x_1)$ and $\beta_2 = B_2(x_1)$ are said to be equal for the domain p_i when and only when $B_1(x) - B_2(x)$ is divisible by $f_i(x)$.

We thus have s new rings $R(p_i, x_1)$ $(i = 1,2,3,\text{----},s)$ such that each number of $R(p,x_1)$ is for the domain of p_i equal to some number of $R(p_i, x_1)$ and the sum, difference, and product of two numbers of $R(p,x_1)$ is for the domain of p_i equal to the sum, difference, and product respectively of the corresponding numbers of $R(p_i, x_1)$. Evidently $f_i(x_1) = 0 \ (p_i)$

We shall next see that these p -adic values of the numbers of $R(p,x_1)$ constitute a domain. We need only show that every number $\beta \not\equiv 0 \ (p_i)$ has a uniquely determined reciprocal in $R(p_i,x_1)$.

Let us therefore suppose that $\beta = B(x_1) \not\equiv 0 \ (p_i)$. Since $\beta \not\equiv 0 \ (p_i)$ it follows that $B(x)$ is not divisible by $f_i(x)$ and hence since $f_i(x)$ is irreducible we know that they are relative prime. Hence there are two polynomials $\psi_i(x)$ and $\phi_i(x)$ such that

$$\phi_i(x) \cdot f_i(x) + \psi_i(x) \cdot B(x) = 1 \ (p)$$

and since rational numbers are equal for the domain of p_i, we can write

$$\phi_i(x) \cdot f_i(x) + \psi_i(x) \cdot B(x) = 1 \ (p_i)$$

the coefficients of the polynomials being rational numbers. But

$$f_i(x_1) = 0 \ (p_i)$$

and hence $\psi_i(x_1) \cdot \beta \equiv 1 \ (p_i)$. Therefore β has a reciprocal which is unique, for if β_1 and β_2 are two numbers such that $\beta \cdot \beta_1 = \beta \cdot \beta_2 = 1 \ (p_i)$, then $\beta\beta_1 - \beta\beta_2 = \beta(\beta_1 - \beta_2) = 0 \ (p_i)$ and hence $\beta_1\beta(\beta_1 - \beta_2) = \beta_1 - \beta_2 = 0 \ (p_i)$. Therefore $\beta_1 = \beta_2 \ (p_i)$ and the p -adic values of the numbers of $R(p,x_1)$ form a domain which we shall denote by $k(p_i,x_1)$.

In $k(x_1)$ p is divisible by $\underline{s}$ distinct prime divisors $p_{i1}, p_{i2}, p_{i3}, \text{------}, p_{is}$, where the notation is so chosen that $f_j(x_i) = 0 \ (p_{ij})$. Since in $k(p)$ x_i cannot satisfy an equation of degree less than n and since $f_j(x) \ (j=1,2,3,\text{-----},s)$ are all distinct, $f_j(x_i) \not\equiv 0 \ (p_{ik}) \ (k \neq j)$. But $f_1(x_i) \cdot f_2(x_i) \cdot \text{-----} f_s(x_i) = 0 \ (p)$ and hence $f_1(x_i) \cdot f_2(x_i) \cdot \text{-------} \cdot f_s(x_i) = 0 \ (p_{jk}) \ (i=1,2,\text{---},n) \ (j=1,2,\text{-}s) \ (k=1,2,\text{-----},s)$.

Let us consider the array I constructed with the various distinct prime divisors of p in each of the n domains $k(x_i)$

$(i=1,2,3,\text{------},n)$ in which each row contains the distinct prime divisors of p in a certain one of the domains.

$$\text{I}\qquad \begin{matrix} p_{11}, p_{12}, p_{13}, p_{14}, \text{--------}, p_{1s} \\ p_{21}, p_{22}, p_{23}, p_{24}, \text{--------}, p_{2s} \\ \text{----------} \\ p_{n1}, p_{n2}, p_{n3}, p_{n4}, \text{--------}, p_{ns} \end{matrix}$$

and associated with this the array of ns numbers from the domains

$$\text{II}\qquad \begin{matrix} f_1(x_1), f_2(x_1), f_3(x_1), \text{---}, f_s(x_1) \\ f_1(x_2), f_2(x_2), f_3(x_2), \text{---}, f_s(x_2) \\ \text{----------} \\ f_1(x_n), f_2(x_n), f_3(x_n), \text{---}, f_s(x_n). \end{matrix}$$

We observe that this arrangement has been so made that any element in II is zero for the domain of the corresponding element of I.

Let us next suppose that $F(V)=0$ is the Galoisian resolvent of $f(x)=0$ for the domain $R(1)$, and that V is any one of its roots. It's degree we shall suppose to be g and when we need to distinguish between the roots we shall denote them by $V_1, V_2, \text{----}, V_g$. The substitutions on the n roots by which these V's are derived from V_1 form a transitive group G of order g. The distinct prime divisors of p in $k(V)$ we shall denote by $P_1, P_2, P_3, \text{------}, P_t$. Since $k(x_1)$ is included in $k(V)$ we see that $t \geq s$.

Let us suppose that in $k(p)$

$$F(V)=F_1(V)\cdot F_2(V)\cdot F_3(V).\text{---------}.F_t(V) \quad (p)$$

where $F_i(V)$ is of degree H_i, and $F_i(V)=0 \ (P_i)$ $(i=1,2,3,\text{-----},t)$. And since the factors are all irreducible, they are all distinct and only one of them is zero for the domain of (P_i) according to

the same discussion as in the case of $f(x)=f_1(x).f_2(x).\text{-----}.f_s(x)(\rho)$ Hence each V_i is a root of some $F_k(V)=0\ (P_\lambda)$ and since this equation cannot have more roots than its degree we know that at most H_k of the numbers $V_1, V_2, V_3, \text{----}, V_g$ are roots of $F_k(V)=0$ where H_k is the degree of $F_k(V)$. Since this is true for all V_i $(i=1,2,\text{----},g)$ and for all $F_k(V)$ $(k=1,2,\text{---},t)$ and since $H_1+\text{--}+H_t=g$ we know that each of the equations $F_k(V)=0\ (P_\lambda)$ $(k=1,2,\text{-----},t)$ has in the domain $k(P_\lambda,V)$ exactly H_k roots.

Let S be a substitution of G which transforms V_1 into V_i and let us suppose that $F_k(V_1)=0\ (P_\lambda)$. The substitution S then transforms $F_k(V_1)$ into $F_k(V_i)$ and this is again zero for the domain of some P_μ. If $F_k(V_i)=0\ (P_\lambda)$ then $\mu=\lambda$. In this case we shall say that S transforms the prime divisor P_λ into the prime divisor P_λ, or the substitution S leaves P_λ invariant. If however $F_k(V_i)\neq 0\ (P_\lambda)$ but $F_k(V_i)=0\ (P_\mu)\ \mu\neq\lambda$ we shall say that S transforms the prime divisor P_λ into the prime divisor P_μ.

Hence every substitution of G either leaves P_λ invariant or transforms it into another prime divisor of p in k(V).

If we now consider that

$$F_1(V).F_2(V).\text{-------}.F_\tau(V)=(V-V_1)(V-V_2)\text{----}(V-V_g)(P_\lambda)$$

and factorization of a polynomial in a domain is unique we know that

$$\begin{aligned}
F_1(V)&=(V-V_{11})(V-V_{12})(V-V_{13})\text{------}(V-V_{1H_1}) \quad (P_\lambda)\\
F_2(V)&=(V-V_{21})(V-V_{22})(V-V_{23})\text{------}(V-V_{2H_2}) \quad (P\ )\\
&\text{----------}\\
F_\tau(V)&=(V-V_{\tau 1})(V-V_{\tau 2})(V-V_{\tau 3})\text{------}(V-V_{\tau H_\tau}) \quad (P_\lambda).
\end{aligned}$$

The substitutions of G which leave P_λ invariant form a

subgroup of G of order say g_1. Let us call this subgroup G_1. The substitutions of G_1 form a group, since G contains all the substitutions which when operated on V_{i1} gives all the other V's, it then contains all the substitutions which when operated on V_{i1} gives all the roots of $F_i(V)$ in P_λ and by hypothesis all these substitutions are in G_1, thus from the theorem in group theory these substitutions of G form a group*.

Every substitution of G transforms each V_i into some V_j $i \neq j$ unless the substitution is the identical substitution because each V_i is a primitive number of k(V) and hence under any substitution S goes over into one of its conjugates since k(V) is a galois field or domain.

Let us suppose that $H_1 \geqq H_i$ $(i=1,2,\text{-----},t)$ and $1, S_2, \text{-----}, S_{H_1}$ are substitutioms such that S_i operating on V_{11} gives V_{1i}. Let us represent this operation as $1V_{11}=V_{11}$, $S_2V_{11}=V_{12}$, $S_3V_{11}=V_{13}$, ---, $S_{H_1}V_{11}=V_{1H_1}$. Thus there are at least H_1 substitutions that leave P_λ invariant. Hence the order of G_1 is $\geqq H_1$. Moreover P_λ cannot be left invariant by any other substitution of G because if such were the case then this substitution S transforms V_{11} into V_{1i} and since S_i and S both transform V_{11} into V_{1i} and $S_i^{-1}S$ leaves V_{11} invariant. But this is as we have said above, only true when $S_i^{-1}S$ is the identical substitution or when $S_i^{-1}S=1$ or $S_i=S$. Hence the order of G_1 is H_1.

G contains at least t-1 substitutions which do not leave P_λ invariant, namely the substitutions which carry V_{11} over into V_{i1} $(i=1,2,\text{----},t)$ or $t_2V_{11}=V_{21}$, $t_3V_{11}=V_{31}$, -----, $t_tV_{11}=V_{t1}$. Then t_2G_1 consists of H_1 substitutions which do not leave P_λ invariant, for

*Miller, Blichfeldt, and Dickson 'Finite Groups' page 286.

since G_1 leaves P_λ invariant it will give a root of $F_2(V)=0\ (P_\lambda)$ when operating on V_{21}, and all of these roots are distinct from those of $F_1(V)$, therefore t_2G_1 transforms P_λ into another prime divisor. The same argument holds with t_3G_1, t_4G_1, ----, $t_\tau G_1$. Thus G contains at least H_1 substitutions that leave P_λ invariant, and $(t-1)H$ substitutions that will transform P_λ into some other prime divisor. Therefore G contains at least tH_1 substitutions, that is $g \geqq tH_1$. Since $g=H_1+H_2+H_3+\cdots\cdots+H_\tau$ and H_1 is $\geqq H_i$ $(i=1,2,3,\cdots,t)$ we see that $g \leqq tH_1$. We therefore conclude that $g=tH_1$ and $H_1=H_2=H_3=\cdots=H_\tau$ Hence $F_1(V)$, $F_2(V)$, $F_3(V)$,-----,$F_\tau(V)$ are all of the same degree, and the substitutions of G_1 permutes the V_{ij} in III with the same first subscript among themselves.

Since G(V) of degree n!, and whose roots are derived from the n! valued function of V_1 is reducible in k(p), and $F_1(V)$ is that irreducible factor in k(p) for which $F_1(V_1)=0\ (P_\lambda)$, the substitutions on x_1, x_2, x_3, -----, x_n by which the roots of $F_1(V)=0\ (P_\lambda)$ are derived from V_1 is called the group of the given equation in k(p).

Since $k(x_1)$ is included in k(V)

$$f_1(x)=(x-x_{11})(x-x_{12})(x-x_{13})\cdots\cdots(x-x_{1n_1})=0\ (P_\lambda)$$

$$f_2(x)=(x-x_{21})(x-x_{22})(x-x_{23})\cdots\cdots(x-x_{2n_2})=0\ (P_\lambda)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$f_s(x)=(x-x_{s1})(x-x_{s2})(x-x_{s3})\cdots(x-x_{sn_s})=0\ (P\lambda)$$

where x_{ji} $(j=1,2,3,\cdots,s)$ $(i=1,2,3,\cdots\cdots,n_i)$ is some one of the roots of $f(x)=0$. The coefficients of $f(x)=f_1(x)\cdot f_2(x)\cdots\cdot f_s(x)$ being symmetric functions of x_{ki} $(k=1,2,\cdots,s)$ $(i=1,2,\cdots,n)$ are unaltered numerically by the substitutions of G_1, because G_1

leaves P_λ invariant, and hence equals numbers in R. It has been shown that G_1 contains all the substitutions that leave P_λ invariant.

Since the roots of $f_i(x)=0$ (P_λ) are x_{i1}, x_{i2}, x_{i3}, ----, x_{in_i} and the roots of $f_i(x)$ in k(p) are, say y_{i1}, y_{i2}, y_{i3}, -----, y_{in_i}, and from the simple isomorphism that exists between the roots in k(p) and those in P_λ, we see that the element x_{ji} in the substitutions of G_1 can be replaced by y_{ji}, and we have the group of f(x) in k(p) in terms of the roots of f(x)=0 in k(p).

Thus the Theorem: If f(x)=0 is irreducible in R(1) and its group in R is G, then in k(p) the group of $f(x)=f_1(x)\cdot f_2(x)\, f_3(x)\cdot\text{------}\cdot f_5(x)$ (p) is simple isomorphic to a subgroup G_1 of G.

Since this group is simple isomorphic to a subgroup of G, we shall discuss some of the properties of this subgroup instead of the group in k(p).

Since f(x) is irreducible in R(1) its group is transitive in the n roots. If f(x) is irreducible in k(p) its group will be transitive also. Thus in this case G_1 is G or a transitive subgroup of G. If f(x) is reducible in k(p) its group is intransitive in the n roots. Since $f_1(x)$, $f_2(x)$, $f_3(x)$, -----, $f_5(x)$ have no common roots, and are irreducible in k(p), the groups of $f_1(x)$, $f_2(x)$, $f_3(x)$, ----, and $f_5(x)$ will not have any common element and will be transitive in their roots. G_1 being the group of f(x)=0 in k(p) it will be composed of these transitive constituents.

If G is a regular group then in k(p) all of the factors of f(x) will be of the same degree, because a subgroup of a regular group will have cycles all of the same degree.

If the group G is not regular, then all of the substitutions do not contain all of the letters, and from a theorem* in group theory, that the order of the sobgroup of a transitive group formed by all of the substitutions which omit a given letter is equal to the order of the group divided by its degree. Hence in this case the order of the group of $f_1(x)$, $f_2(x)$, $f_3(x)$, ---, and $f_s(x)$ separately can not exceed g/n, that is, the order of the transitive constituents can not exceed g/n. Likewise if in k(p) f(x) has one linear factor, this root will not be an element of G_1, and therefore G_1 will be of order g/n. If there are several linear factors in k(p) the order of G_1 may be less.

Since $F_i(V)$ (i=1,2,3,----, or t) is irreducible in k(p), if the discriminant of $F_i(V)$ is not divisible by p, from the theory of p-adic numbers, we have that the roots of $F_i(V)=0 \bmod p$ are V_{i1}, V_{i1}^{p}, $V_{i1}^{p^2}$, ----, $V_{i1}^{p^{H_i-1}}$. If $SV_{i1}=V_{i1}^{p}$ then $S^2V_{i1}=SV_{i1}^{p}=(SV_{i1})^{p}=V_{i1}^{p^2}$, etc. Thus the group G_1 is cyclic and thus transitive. Therefore f(x) has all linear factors but one of degree G_1, and since G_1 does not contain all the roots its order is g/n, or a subgroup of this group of order g/n.

If the group of f(x)=0, f(x) being irreducible in R(1), is known, then by studying the subgroups of G one can form some idea of the factors of f(x)=0 in k(p), and in many cases determine exactly the form of the factors, as in the case when G is regular.

By extending this work it may be possible to determine the exact subgroup for certain classes of p and thus determine exactly the factors of f(x) in k(p) from the group standpoint of view.

*Miller, Blichfeldt, and Dickson 'Finite Groups' page 32.